BY ORDER OF THE
INSTALLATION COMMANDER

CHARLESTON AIR FORCE BASE
MANUAL 37-1

1 APRIL 1995

Information Management

437TH AIRLIFT WING NETWORKING POLICIES

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: 437 MSS/IMX ( )

Certified by: 437 MSS/IM
(Captain David J. Hluska)
Pages: 5
Distribution: F

This manual outlines responsibilities and provides information and policy for Wide Area Network (WAN), Metropolitan Area Network (MAN), and Local Area Network (LAN) users, Work Group Managers (WGM), the 437 AW, and Charleston AFB. This document serves as the user's passport to the LAN. This manual includes policy for use of electronic mail (E-mail), system security, standard office automation suite and other basic network services and allows users to electronically manage information throughout its life cycle.

1. Applicability. This manual applies to personnel who use or support the 437 AW network hardware or software. It covers the use of all components of the 437 AW MAN including users, information, peripherals, software, and computing and networking equipment that are not connected to the MAN but are connected to and communicating to any other computer which creates a LAN.

2. Responsibilities.

2.1. Users: All personnel are to use the networks in a responsible manner and within all applicable policies and directives. Every effort will be made to utilize the networks to the fullest extent possible while enjoying the benefits of reduced paper consumption, shared hardware and legally licensed software resources, and efficient communications. Users are the primary customers of the networks. They should responsibly articulate information needs and system needs to their Business Processes Representative or Unit System Administrator (USA) as appropriate.

2.2. Business Processes Representative: Every unit connected to the MAN or possessing an internal LAN should appoint a Business Processes Representative. This person should be very familiar with information needs of the users. An individual who works with LAN provided information (e.g. orderly room workers, administration section heads, secretaries, etc.) is ideal for this position. Information needs consist of future requirements based on mission, goals, and objectives. An information need may also be an idea for an enhancement that improves the system's utility or increases productivity. Business Processes Representatives will meet corporately, each quarter minimally, as the Business

Processes Working Group (BPWG). Each Group will have two members in attendance. They are responsible to their constituency for all information needs.

2.3. Unit System Administrator: Every unit connected to the MAN or possessing an internal LAN should appoint a USA. This person should be very familiar with the system needs of the users. System needs require attention in order to operate within the current system configuration. The person who acts as the unit's local domain administrator (provides access to the LAN, sets up passwords, manages local applications software, arranges and conducts training) is the ideal choice for this position. USAs will meet corporately each month as the Configuration Control Board/Technical Working Group (CCB/TWG). The user will pursue resolution of all system needs through their USA. USAs must ensure users read this entire manual before assigning passwords and granting access. The USA should brief newly assigned personnel on their responsibilities during initial in-processing. More specific USA responsibilities are:

Install server and workstation software	Maintain List of E-mail users for their unit
Report E-mail changes to post office manager	POC to the BNCC
Diagnose troubles at their local network	Maintain TCP/IP addresses database
Ensure computer names are standard	Insure logon names are standard
Train workstation users	Attend necessary training
Budget for LAN upgrades	Install/configure all software on server and workstation
Scan workstation and server for virus	Password accountability
Workstation and server security	Backup servers
Contingency Planning & Disaster Recover Software	License and metering
Manage Workgroup files and processes	Maintain network maps of their building

Prepare all 3215 requests for network hardware and software acquisition

2.4. Base Information Management (IM): IM is the focal point for ensuring network users' information needs are being met. The primary vehicle for this is the quarterly BPWG meeting which is chaired by IM. This group is responsible for identifying, clarifying, tracking, and endorsing (or opposing) information requirements. Special emphasis will be on information flow, compliance with regulations for E-Forms, written correspondence, document security, Privacy Act, Freedom of Information Act (FOIA), reduction of paper, and electronic record keeping. Issues and needs identified at the meeting are opened as action items and sent to the CCB/TWG. IM is also a member of the CCB/TWG.

2.5. Communications Squadron (CS): CS is responsible for ensuring all networks operate within established policies and procedures and delegating appropriate functions to the Unit System Administrators. CS oversees MAN resources (file server, communications architecture components, and network software), conducts system maintenance, chairs CCB/TWG meetings, provides a representative to the BPWG, and manages connectivity and MAN/WAN level resources, i.e., Domain Name Service, Mail Gateway, Mail Transfer Agent, Gateway Post office, TCP/IP addresses, etc.

3. Security.

3.1. Security is everyone's responsibility. Information security, software security, and physical security are three types of network security. AFPD 33-2, *C4 Systems Security*, details Air Force Computer Security Policy. Users are responsible for backing up their data. Additionally, physical security of the equipment and storage media is the responsibility of the individual office. See AFSSI 5013, *Password Management*; 5100, The Air Force Computer Security (COMPUSEC) Program, and AFSSM 5019, *Computer Security User's Guide*; 9000, C4 Systems Security Glossary, for more details.

3.2. Network security objectives are to (1) prevent, (2) detect, and (3) recover from system threats. Prevention is the first line of defense. If that fails, the next step is to attempt to detect the intrusion. As a last resort, recovery must be available. Backups are a vital part of the user's security procedures. Report security violations to your Computer Security Officer (CSO) immediately. Report violations of this manual to your Unit System Administrator.

3.3. Treat passwords as being equivalent to signatures. Allowing others to learn passwords is giving them permission to freely sign documents for others. Do not write passwords in conspicuous places (i.e. place mats, bottom of phones, Rolodex, Post It Notes, etc.). Memorize them. Change passwords periodically or at least semiannually.

3.3.1. USAs will immediately remove log-in and passwords of users who terminate their employment, PCS, or PCA. After signing on the network, all users are responsible for protection access from unauthorized individuals. If your terminal is left unattended, ensure you log out of the network or use a password protected screen saver.

3.3.2. All users will use unique passwords (combination of upper case, lower case, and non-alpha numeric). Once the password is used, it should not be used again. Minimum password length: 6 characters alpha/numeric combination. Do not use obvious passwords such as nicknames, family names, phone numbers, address/office symbols, or words found in the dictionary.

3.4. Account lock-out. When attempting to log into the network, all users will be given three attempts to correctly input their password. The third unsuccessful attempt "locks" the account, requiring work USA assistance.

3.5. A combination of software programs and procedures is necessary to protect wing network assets from viruses. Users are required to scan all floppy disks they bring in from home or off-base. 437 CS is responsible for providing virus protection software on the file servers. This anti-virus software will continuously and automatically scan all files coming into or out of the servers for viruses. Additionally, the software scans all users' PCs weekly for viruses.

3.6. Information is the most valuable part of any information system. Users should frequently back up their important files by saving information to both the file server and to their local drive or tape back up. USAs are responsible for ensuring daily tape backups of the file servers. Additionally, 437 CS has implemented disaster prevention recovery procedures, established fault tolerance, and minimized server problems, ensuring uninterrupted operation.

3.7. Nonstandard peripherals connected to any part of the MAN or organizational LAN must be approved by 437 CS prior to installation.

4. Electronic Mail (E-Mail) and Electronic Correspondence.

4.1. E-Mail provides an electronic communication capability which follows the general procedures used for processing paper correspondence. E-mail requires protection, safeguarding, and is subject to

the Privacy Act. Official correspondence sent through the e-mail communication system must follow the general format of AFMAN 37-126, *Preparing Official Communications*, and CAFBR 11-8, *Charleston Air Force Base Guide for Preparing Written Communications*. It must observe traditional customs and courtesies, and be unclassified (except where approved by 437 CS). Use the official chain of command when addressing E-mail to senior officers.

4.2. Electronic correspondence meets the requirements of AFH 37-137, *Tongue and Quill*. Examples are letters, staff summary sheets, attachments, memoranda, short notes, and messages. Release of formal correspondence electronically carries implied authentication and signature. Personnel will **NOT** send E-mail using any log-in other than that specifically assigned to them by their USA. The E-mail system automatically attributes the source of the correspondence based on the LOG-IN and PASSWORD. Messages need not be followed by paper copy except in cases where official record copies must be maintained.

4.3. Message content must be of official business and unclassified (except where approved by 437 CS). Private mail will be minimized and should be confined to subject matter relating to government business. Section activities and morale issues are acceptable subject matter. Discretion must be exercised in sending several types of sensitive information such as Privacy Act or For Official Use Only (FOUO). (See AMCR 4-2, *Electronic Mail for Office Information Systems/Network*, for a complete listing.).

4.4. Use electronic mail and the network infrastructure as an alternative to traditional hand-carry coordination processes. E-mail should be used ahead of the Base Information Transfer System (BITS), US Postal Service, or Facsimile (FAX). Staffing/coordination actions can be accomplished via E-mail, reducing printing time and associated costs.

5. E-Mail as Official Records. Organizational correspondence requires filing of hard copy in accordance with AFI 37-122, *Air Force Records Management Program*, and AMCR 4-2. Keep an E-mail message if the following circumstances exist: contains information developed in preparing position papers, reports, or studies; reflects official actions taken in the course of conducting agency business; conveys statements of policy or the rationale for decisions or actions; documents oral exchanges during which policy or agency activities were discussed or formulated; includes calendars or information from external communications systems. Do not keep E-mail messages about retirement ceremonies, luncheons, office picnics etc. The originator is responsible for keeping the record copy. Network storage limitations may require transfer of E-mail messages to another medium such as computer hard drive, floppy disk, magnetic tape, or paper. Compliance with Federal laws governing records management is mandatory regardless of the storage medium.

6. Other Network Applications. There are numerous applications available via the networks. For information about accessing these and other services, contact your Unit System Administrator. USAs should see the BNCC staff for more information on accessing these services.

HENRY L. HUNGERBEELER, Colonel, USAF
Commander, 437th Support Group

ATTACHMENT 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 37-122, *Air Force Records Management Program*

AFPD 33-2, C4 Systems Security

AFMAN 37-126, *Preparing Official Communications*

AFSSI 5013, *Password Management*

AFSSM 5019, *Computer Security User's Guide*

AFH 37-137, *Tongue and Quill*

AMCR 4-2, *Electronic Mail for Office Information Systems/Network*

CAFBR 11-8, *Charleston Air Force Base Guide for Preparing Written Communications*

Abbreviations and Acronyms

BPWG—Business Processes Working Group

CCB/TWG—Configuration Control Board/Technical Working Group

CS—Communications Squadron

IM—Information Management

LAN—Local Area Network

MAN—Metropolitan Area Network

USA—Unit System Administrator

WAN—Wide Area Network